Brad Stewart, Kalaseel
703 205 8000
Ulf Dahl
104-591 0
171

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) Sökande *Anonymity Protection in Sweden AB, Göteborg SE*
Applicant (s)

(21) Patentansökningsnummer *9602475-7*
Patent application number

(86) Ingivningsdatum *1996-06-20*
Date of filing

Stockholm, 1998-02-10

För Patent- och registreringsverket
For the Patent- and Registration Office

Åsa Dahlberg
Åsa Dahlberg

Avgift
Fee *170:-*

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

AWAPATENT

ANONYM DATA PROTECTION IN SWEDEN AB

Handläggare
Sören Giver/MY

Fane

Referens
2951296

METOD FÖR DATABEARBETNING

Tekniskt område

Föreliggande uppfinning hänför sig till teknikområdet datorstödd informationshantering, och avser närmare bestämt en metod för databearbetning enligt ingressen till patentkravet 1 för åstadkommande av utökat skydd mot obehörig bearbetning av datainformation.

Teknisk bakgrund

Inom teknikområdet datorstödd informationshantering föreligger det starka krav på ett utökat skydd mot obehörigt intrång i datorregister, i synnerhet mot obehörigt intrång i den enskildes personliga integritet vid inrättande och förande av personregister, dvs register som innehåller upplysningar om enskilda personer. Härvid föreligger det speciellt restriktioner och förbud mot så kallad samkörning av personregister. Även inom andra områden, såsom näringsliv, försvar, bankväsen, försäkringar, etc, föreligger det en efterfrågan på ett bättre skydd mot otillbörligt intrång i de verktyg, databaser, tillämpningar, etc som används för administrering och lagring av känslig datainformation.

WO95/15628, med samma innehavare som föreliggande ansökan, beskriver en datalagringsmetod som ger ökade möjligheter till samkörning utan risk för reducerad integritet. Metoden, som illustreras schematiskt i fig 1 och 2 på bifogade ritningsblad, avser lagring av datainformation innefattande dels en identifierande information eller originalidentitet OID, exempelvis personnummer Pnr, dels tillhörande beskrivande information BI. Datainformationen OID + BI lagras som poster P i en

databas O-DB enligt följande princip:

Steg 1 OID (Pnr) krypteras medelst en första, företrädesvis icke-reversibel algoritm ALG1 till en uppdateringsidentitet UID;

Steg 2 UID krypteras medelst andra, reversibel algoritm ALG2 till en lagringsidentitet LID;

Steg 3 LID och BI lagras som en post P i databasen O-DB, varvid LID fungerar som postidentifierare;

Steg 4 Vid förutbestämda tidpunkter åstadkommes (se fig 2) en ändring av LID hos alla eller utvalda poster P genom att LID hos dessa poster dekrypteras medelst en dekrypteringsalgoritm ALG3 till UID, varefter efter UID krypteras medelst en modifierad andra, reversibel algoritm ALG2' till en ny lagringsidentitet LID', som införs som ny postidentifierare i respektive post P som ersättning för tidigare LID. Därmed åstadkommes en säkerhetshöjande "flytande" ändring av LID hos posterna.

För en närmare beskrivning av detaljerna och fördelarna hos denna krypterings- och lagringsmetod hänvisas till WO95/15628, vilket dokument skall anses utgöra del av föreliggande beskrivning. Lagringsprincipen enligt steg 1-4 ovan benämns i det följande PTY, vilket är en förkortning av konceptet PROTEGRITY som står för "Protection and Integrity".

En utförlig teknisk beskrivning av PTY ges vidare i dokumentet "PROTEGRITY (ASIS) Study 2", Ver 1.2, 1 mars 1996, av Leif Jonson. Även detta dokument skall anses utgöra del av föreliggande beskrivning.

Inom det aktuella teknikområdet är dock så kallade skalskydd idag den dominerade skyddsmetoden. Skalskydd omfattar dels den yttre säkerheten (lokaler), dels ett behörighetskontrollsystem (BKS) med användar-lösenord

för åtkomststyrning. BKS används som skalskydd för stordatorer, client/server-system och PC, men det ger inte något fullgott skydd, och den aktuella datainformationen kan ofta relativt lätt utsättas för obehörig åtkomst. Detta skydd har visat sig vara allt mer otillfredsställande, då man i allt större omfattning lagrar "känslig" datainformation som måste kunna hanteras via distribution, lagring och bearbetning i dynamiskt skiftande miljöer, särskilt lokal distribution ut till persondatorer. I takt med denna utveckling blir systemgränserna allt otydligare och försämras den effekt som ett skalskydd kan ge.

Sammanfattning av uppfinningen

Med bakgrund av ovanstående har föreliggande uppfinning som ändamål att åstadkomma en förbättrad metod för bearbetning av datainformation, med vars hjälp man kan höja säkerheten mot otillbörlig åtkomst till känslig datainformation.

Ett särskilt ändamål hos uppfinningen är att anvisa en teknik för databearbetning- eller hantering som gör det möjligt för systemansvarig, organisationens ledning eller motsvarande att på ett enkelt sätt fastställa och kontinuerligt anpassa användarsidans möjligheter att bearbeta lagrad datainformation som skall skyddas.

Ytterligare ett ändamål hos uppfinningen är att anvisa en teknik för databearbetning som erbjuder skydd mot försök till obehörig databearbetning med hjälp av icke godkänd programvara.

Annu ett annat ändamål hos uppfinningen är att anvisa en teknik för databearbetning enligt ovan angivna ändamål, som kan användas i kombination med ovan beskrivna PTY-princip för åstadkommande av ett säkerhetssystem med extremt hög skyddsnivå.

Dessa och andra ändamål hos uppfinningen uppnås med metoden enligt patentkravet 1, varvid föredragna utfö-

ringsformer av uppfinningen är angivna i de osjälvständiga patentkraven.

Sålunda anvisas enligt uppfinningen en metod för bearbetning av data som skall skyddas, innefattande åtgärden att lagra datat som krypterade termvärden hos poster i en första databas (O-DB), varvid varje termvärde är kopplat till ett motsvarande termnamn.

Metoden enligt uppfinningen kännetecknas av följande ytterligare åtgärder:

att i en andra databas (IAM-DB) lagra en termskyddskatalog, som för varje enskilt termnamn innehåller ett eller flera skyddsattribut som anger bearbetningsregler för de termvärden som i den första databasen är kopplade till det enskilda termnamnet,

att vid varje användarinitierad åtgärd, som syftar till bearbetning av ett givet termvärde i den första databasen, initialt åstadkomma ett tvingande anrop till termskyddskatalogen för inhämtning av det eller de skyddsattribut som hör till motsvarande termnamn, och att tvingande styra bearbetningen av det givna termvärdet i överenstämmelse med det eller de inhämtade skyddsattributen.

I föreliggande ansökan gäller följande definitioner:

- "Bearbetning" kan inkluderar alla åtgärdstyper som innebär någon form av läsning, skrivning, ändring, kodning, förflyttning, kopiering, etc. av data som skall skyddas med metoden enligt uppfinningen.
- "Termnamn" avser en specifik typ av data med överenskommen innebörd.
- "Termvärde" avser ett värde som i en given post specificerar ett termnamn.
- "Post" avser ett antal samhörande termvärden kopplade till respektive termnamn, eventuellt även innefattande en postidentifierare med vars hjälp posten kan identifieras. Exempel:

	TERMNAMN	
POST-ID	SOCIALBIDRAG	BIL
XXXX XXXXX	krypterat termvärde	krypterat termvärde
YYYY YYYYY	krypterat termvärde	krypterat termvärde

- "Skyddsattribut som anger bearbetningsregler" kan avse:
  - i termskyddskatalogen lagrade datauppgifter som i sig ger fullständig information om den eller de regler som gäller för bearbetning av motsvarande term, och/eller
  - i termskyddskatalogen lagrade datauppgifter som kräver ytterligare anrop till på annan plats lagrad information som, eventuellt i kombination med skyddsattributen, anger de aktuella bearbetningsreglerna.

- "Inhämtning av skyddsattribut" kan avse:
  - inhämtning av skyddsattributen i den form de är lagrade i termskyddskatalogen, och/eller
  - inhämtning av data som utvinns från skyddsattributen, exempelvis genom dekryptering därav.

- "Kryptering" kan avse vilken som helst form av kryptering, trikryptering, omvandling eller kodning av klartext-data till icke-tolkningsbar (krypterad) data, och skall speciellt också avse omvandlingsmetoder som inkluderar hashning.

Den uppfinningsenliga metoden erbjuder en ny typ av skydd, som skiljer sig väsentligt från det kända skalskyddet, och som verkar på cell- eller termnivå. Till varje termnamn som används i posterna i den första databasen hör sålunda ett eller flera skyddsattribut, vilka är lagrade i en separat termskyddskatalog och vilka skyddsattribut anger regler för hur bearbetning av mot-

svarande termvärden skall ske. Det skall särskilt noteras att anropet till termskyddskatalogen är tvingande. Detta betyder att ett system, i vilket metoden enligt uppfinningen är implementerad, är sådant att en användare, som vill exempelvis läsa ett visst termvärde i en given post i den första databasen, genom sitt försök till åtkomst till termvärdet automatiskt och tvingande åstadkommer ett systemanrop till termskyddskatalogen i den andra databasen för inhämtning av de skyddsattribut som hör till motsvarande termnamn. Systemets fortsatta bearbetningsprocedur (utläsning av termvärde) styrs också tvingande i enlighet med det eller de inhämtade skyddsattribut som gäller för motsvarande termnamn.

Begreppet "termskyddskatalog" och användningen därav enligt föreliggande uppfinning får ej förväxlas med det kända begreppet "active dictionary", som innebär att det utöver en operativa databas finns en särskild tabell vilken anger olika definitioner eller val för termvärden i den operativa databasen, exempelvis att ett termvärde "gul" definitionsmässigt innebär en färgkod som ligger inom ett i en sådan uppslagstabell angivet numeriskt intervall.

Det är föredraget att de av skyddsattributen angivna bearbetningsreglerna är oåtkomliga för användarsidan, och att de avlästa eller inhämtade skyddsattributen endast används internt av systemet för styrning av bearbetningsprocessen. En given användare, som exempelvis vill läsa ut i databasen lagrad information om en viss individ, behöver sålunda inte alls vara medveten om att vissa skyddsattribut har aktiverats och medfört att viss, känslig information för denna individ har uteslutits i den information som görs tillgänglig på exempelvis en bildskärm. Varje användarinitierad åtgärd som syftar till bearbetning av termvärden medför sålunda dels ett tvingande anrop till termskyddskatalogen och dels en fortsatt bearbetning som är tvingande underkas-

tad de bearbetningsregler som anges av skyddsattributen, och detta kan sålunda åstadkommas utan att användaren får information om vilka regler som styr den aktuella bearbetningen, och speciellt att användaren inte heller har möjlighet att få åtkomst till reglerna.

Genom att ändra, lägga till och ta bort skyddsattribut i termskyddskatalogen kan systemansvarig eller motsvarande enkelt bestämma, för varje enskilt termnamn, de bearbetningsregler som gäller för termvärden som hör till det enskilda termnamnet och därmed enkelt upprätthålla en hög och överskådlig säkerhetskvalitet i systemet.

Sålunda gäller enligt uppfinningen att det är den enskilda termen (termnamnet) och inte hela register, som blir styrande enhet för hur systemansvarig organisation, operatör, etc, har fastställt nivån på kvalitet, ansvar och säkerhet avseende informationshanteringen.

För uppnående av en hög skyddsnivå är det föredraget att kryptera termskyddskatalogen för förhindrande av otillbörlig åtkomst till densamma.

Som föredragna skyddsattribut anvisas enligt uppfinningen följande möjligheter, vilka dock endast förses som en icke-uttömmande, exemplifierande lista:

1. Angivande av vilken "styrka" eller "nivå" (t.ex. ingen, 1, 2,...) av kryptering som skall användas för lagring av motsvarande termvärden i databasen. Olika termvärden inom en och samma post kan alltså vara krypterade med inbördes olika styrka.

2. Angivande av vilken "styrka" eller nivå (t.ex. ingen, 1, 2,...) av kryptering som skall användas på motsvarande termvärden om dessa skall överföras på ett nät.

3. Angivande av program och/eller programversioner som är godkända att användas för bearbetning av motsvarande termvärden.

4. Angivande av "ägare" till termnamnet. Olika termvärden inom en och samma post kan sålunda ha olika ägare.

5. Angivande av gallringsregler för motsvarande termvärden, exempelvis angivande av metod och tidpunkt för automatisk borttagning av motsvarande termvärden från databasen.

6. Angivande om automatisk loggning skall ske vid bearbetning av motsvarande termvärden.

Enligt en särskilt föredragen utföringsform av uppfinningen används ovan beskrivna PTY-lagringsmetod för kryptering av allt data som skall krypteras i såväl databasen (dvs termvärdena) som termskyddskatalogen (dvs skyddsattributen). För det normala fallet där varje post har en postidentifierare (svarande mot LID ovan) är det föredraget att även postidentifieraren skyddas med PTY. Speciellt kan därvid en flytande ändring av postidentifierarna i såväl den operativa databasen som termskyddskatalogen utföras med önskade intervaller eller vid slumpmässigt valda tidpunkter, i enlighet med ovan beskrivna PTY-princip. I det föredragna utförandet kan speciellt den inneslutna processör som används för PTY-krypteringen också användas för implementering av anropen till termskyddskatalogen och proceduren för bearbetning enligt inhämtade skyddsattribut.

Uppfinningen skall nu förklaras närmare under hänvisning till bifogade ritningar, som schematiskt åskådliggör den uppfinningsenliga principen implementerad i ett exemplifierande datasystem.

Kort beskrivning av ritningarna

Fig 1 (känd teknik) visar schematiskt principen för lagring av datainformation enligt PTY-principen i WO95/15628.

Fig 2 (känd teknik) visar schematiskt principen för åstadkommande av flytande lagringsidentiteter enligt PTY-principen i WO95/15628

Fig 3 visar schematiskt ett datorsystem för implementering av metoden enligt uppfinningen.

Fig 4 visar schematiskt principen för databearbetning enligt uppfinningen med tvingande anrop till en termskyddskatalog.

Fig 5 visar ett exempel på en skärmbild för bestämning av skyddsattribut i termskyddskatalogen.

Beskrivning av föredraget utföringsexempel

I det följande kommer beteckningen IAM (vilket står för Information Assets Manager) att användas för de komponenter och applikationer som i utföringsexemplet är centrala för implementeringen av uppfinningen.

Först hänvisas till fig 3, som schematiskt åskådliggör ett datahanteringssystem i vilket föreliggande uppfinning är implementerad och i vilket system följande databaser ingår för lagring av datainformation, i detta exempel personrelaterad datainformation:

- En öppen databas Ö-DB som innehåller allmänt tillgängligt data, såsom personnamn, artikellnamn, adress, etc, med personnummer Pnr i klartext som postidentifierare;
- En operativ databas O-DB, vilken innehåller data som skall skyddas. Krypterad identifikation, såsom i detta fall krypterat personnummer, används som postidentifierare (=lagringsidentitet LID). O-DB används av behöriga användare för bearbetning av enskilda poster, såsom läsning och uppdatering;

- En arkiv-databas A-DB, vilken innehåller från den operativa databasen O-DB överfört (gallrat) data och vilken används för statistiska frågor, men inte för frågor riktade mot enskilda poster. Överföringen från O-DB till A-DB kan ske batchvis.
- En databas IAM-DB, vilken är en för implementeringen av uppfinningen central databas. Denna databas innehåller en termskyddskatalog med skyddsattribut för sådana termnamn som hör till termvärden hos poster i den operativa databasen O-DB. Denna databas IAM-DB är företrädesvis fysiskt åtskild från övriga O-DB och är oåtkomlig för användarsidan. Det kan dock föreligga två eller fler uppsättningar av termskyddskatalogen: dels en originalversion som endast behörig IAM-operatör har tillgång till, och dels en kopieversion som importerar termskyddskatalogen från originalversionen och som eventuellt kan ligga på samma lagringsmedium som den operativa databasen O-DB. De två versionerna kan vara fjärrbelägna från varandra, exempelvis i två olika städer.

I datasystemet i fig 3 ingår vidare en hårdvarukomponent 10, en styrmodul 20 (IAM-API), och en programmodul 30 (PTY-API). Funktionen hos dessa tre komponenter skall nu beskrivas närmare.

Hårdvarukomponenten 10

Hårdvarukomponenten 10 fungerar som en egen distribuerad processor i en datamaskin. Den har en innesluting som gör den helt manipuleringssäker, vilket innebär att den inte skall kunna avlyssnas med s.k. traceverktyg.

Hårdvarukomponenten 10 kan som en självständig enhet utföra åtminstone följande funktioner:

- Skapa variabla reversibla och icke-reversibla krypteringsalgoritmer för PTY-krypteringen samt förse dessa algoritmer med erforderliga variabler;
- Initiera förändringar av lagringsidentiteter (LID) hos lagrat data i enlighet med PTY, dels data i O-DB, dels data i termskyddskatalogen hos IAM-DB;
- Lagra handläggarbehörigheter som har tillgång till poster i O-DB; och
- Koppla originalidentiteter OID med rätt post i O-DB.

Styrmodulen 20 (IAM-API)

Styrmodulen styr hanteringen av de typer av dataskydd som systemet kan tillhandahålla.

Styrmodulen utför bearbetningen som begärs via API (Application Program Interface) programmeringsgränssnitt.

Programmodulen 30 (PTY-API) 30

Programmodulen (PTY-API) 30 hanterar dialogen mellan aktuell applikation 40 (inklusive BKS) och hårdvarukomponenten 10. Denna modul kan vidare föra en händelselogg samt styra gallring/borttagning av data från den operativa databasen O-DB.

Nu hänvisas till fig 4, som visar samma fyra databaser (Ö-DB, O-DB, A-DB, IAM-DB) som i fig 3 och som schematiskt åskådliggör hur bearbetningen av enskilda termer, i enlighet med uppfinningen, styrs i enlighet med regler som anges av skyddsattribut i termskyddskatalogen, vilken är lagrad i databasen IAM-DB.

Det data som skall lagras avser i detta exempel en viss individ och innehåller: (1) allmänt tillgängligt data som namn och adress, (2) identifierande information, såsom personnummer, (Pnr), samt (3) beskrivande information BI. Det allmänt tillgängliga datat namn och adress lagras tillsammans med personnummer Pnr i den öppna databasen Ö-DB, vilken lagring kan ske i klartext

eftersom informationen är av allmänt tillgänglig karaktär.

För lagring den identifierande informationen i förening med den beskrivande informationen BI utförs emellertid nedan angivna steg, varvid följande beteckningarna används för beskrivning av krypterings- och dekrypteringsalgoritmer. Krypterings- och dekrypteringsalgoritmerna kan generellt beskrivas enligt följande:

$$F_{Typ}(Slumptal, Indata) = Resultat$$

där:

F betecknar en funktion.

Typ anger funktionstyp enligt följande:
F_{KIR} = Icke reversibel krypteringsalgoritm
F_{KR} = Reversibel krypteringsalgoritm
F_{DKR} = Dekrypteringsalgoritm

Slumptal är en eller flera konstanter och/eller variabler ingående i funktionen F.

Indata utgörs av den datainformation som skall krypteras respektive dekrypteras.

Resultat är ett unikt funktionsvärde för en given funktion.

Steg 1 <u>Uppdelning av datainformationen:</u>
Identifierande information separeras från beskrivande information;

Steg 2 <u>Framtagning av lagringsidentitet LID:</u>
En originalidentitet OID väljs utifrån den identifierande informationen. OID väljs här lika med

individens personnummer Pnr. OID krypteras medelst en av hårdvarukomponenten 10 slumpmässigt framtagen, icke-reversibel krypteringsalgoritm ALG1 till en uppdateringsidentitet UID enligt följande:

$$ALG1: \quad F_{KIR}(\text{Slumptal, OID}) = \text{UID}$$

ALG1 är sådan att man vid försök till dekryptering av UID till OID erhåller ett mycket stort antal identiteter, vilket gör det omöjligt att koppla en viss UID till motsvarande OID.

UID krypteras därefter medelst en reversibel algoritm ALG2, vilken likaså framtages slumpmässigt av hårdvarukomponenten 10, för bildande av en lagringsidentitet LID enligt följande:

$$ALG2: \quad F_{KR}(\text{Slumptal, UID}) = \text{LID}$$

ALG2 är sådan att det existerar en motsvarande dekrypteringsalgoritm ALG3 med vilken LID kan dekrypteras för återskapande av UID.

Lagringsidentiteten LID används, såsom beskrivs i steg 4 nedan, som krypterad postidentifierare vid lagring av krypterade termvärden TV i den operativa databasen O-DB.

Steg 3 <u>Framtagning av krypterade termvärden TV:</u>
Den beskrivande datainformation BI som hör till originalidentiteten OID omvandlas till ett eller flera krypterade termvärden TV kopplade till var sitt termnamn TN.

Krypteringen sker enligt följande med en rever-

sibel krypteringsfunktion F_{KR}, som i likhet med algoritmerna ALG1 och ALG2 ovan också framtages slumpmässigt av hårdvarukomponenten 10. Utmärkande för uppfinningen är att det här sker ett tvingande anrop till termskyddskatalogen i databasen IAM-DB, för automatisk inhämtning av det skyddsattribut som är kopplat till det aktuella termnamnet och som anger den "styrka" eller grad med vilken krypteringen av det beskrivande datat skall utföras för bildande av termvärdet TV.

Den tabell som i fig 4 visas nedanför databasen IAM-DB symboliserar ett exemplifierande innehåll hos termskyddskatalogen, här betecknad med TK. Som exempel kan det här antagas att skyddsfunktionen Funk1 svarar mot "krypteringsgrad". Om den aktuella beskrivande informationen BI skall lagras som ett termvärde hörande till det specifika termnamnet TN1 i termskyddskatalogen, så inhämtas i detta fall automatiskt det i termskyddskatalogen registrerade skyddsattributet "5". Den aktuella, beskrivande informationen BI kommer därigenom, automatiskt och tvingande, att krypteras med styrka "5" för bildande av ett krypterat termvärde TV enligt följande:

F_{KR}(Slumptal, BI) = krypterat termvärde TV

För lagring av en mindre känslig term, exempelvis en term med termnamnet TN3, skulle det tvingande anropet till termskyddskatalogen i IAM-DB istället ha resulterat i att skyddsattributet "nej" inhämtades, varvid någon kryptering ej skulle gjorts på det aktuella beskrivande datat som då kunde lagras i klartext i den operativa databasen O-DB.

Steg 4 Lagring av poster i operativa databasen O-DB: Den krypterade lagringsidentiteten LID enligt steg 2 i förening med motsvarande, krypterade termvärde eller termvärden TV enligt steg 3 lagras som en post i den operativa databasen O-DB.

Enligt ovanstående beskrivning har en lagrad uppgiftspost P i den operativa databasen således följande generella utseende:

	Beskr. information i form av krypterade termvärden			
Lagringsidentitet (LID)	TV1	TV2	TV3	TV4

Originalidentiteten OID krypteras enligt PTY-principen i två steg, av vilka det första är icke reversibelt och det andra reversibelt. Därmed blir det möjligt att å ena sidan lagra den beskrivande informationen BI med en lagringsidentitet LID som aldrig kan kopplas till originalidentiteten OID, och å andra sidan att skapa flytande, dvs i tiden föränderliga, lagringsidentiteter LID, och fortfarande ha möjlighet att vid angivande av en viss originalidentitet OID kunna lokalisera tillhörande, lagrad beskrivande information BI.

Det beskrivande datat BI lagras i enlighet med till varje enskild term kopplade skyddsattribut. Därmed uppnås en än högre skyddsnivå samt en hög grad av flexibilitet beträffande upprättande av regler, och kontinuerlig anpassning av dessa, för hur känsligt data får och kan användas, och detta ända ner på termnivå.

För att höja skyddsnivån ytterligare är det föredraget att lagra termskyddskatalogen TK i IAM-DB i krypterad form i enlighet med PTY-principen, varvid exempelvis termnamnen svarar mot lagringsidentitet ovan och skyddsattributen svarar mot beskrivande information

eller termvärden ovan, såsom schematiskt illustreras i fig 4. Därmed förhindras effektivt varje försök att kringgå termskyddet genom otillbörlig åtkomst och tolkning av innehållet i termskyddskatalogen.

I det illustrerade utföringsexemplet kan PTY sålunda ha följande funktioner:

- Skydda originalidentiteten OID i krypterad form (LID) på den operativa databasen O-DB (såsom är känt från nämnda WO95/15628);
- Skydda datainformation i IAM-DB, i synnerhet termskyddskatalogens skyddsattribut och tillhörande postidentifierare; och
- Skydda beskrivande information BI i form av krypterade termvärden TV för de termnamn som har motsvarande skydd aktiverat i termskyddskatalogen, och i enlighet med motsvarande skyddsattribut. funktionalitet

Funktionalitetsskydd

I ovanstående utföringsexempel av proceduren för inskrivning av data i den operativa databasen O-DB har som termskyddsattribut i termskyddskatalogen TK hittills endast diskuterats "krypteringsgrad". Detta är emellertid endast ett exempel bland flera möjliga skyddsattribut i termskyddskatalogen, vilken normalt erbjuder ett flertal skyddsattribut för varje term. Föredragna skyddsattribut har angivits ovan i den allmänna beskrivningsdelen.

Ett särskilt intressant skyddsattribut är "skyddade program". Användning av detta termskyddsattribut innebär att datasystemet kan erbjuda en ny skyddstyp, vilken här benämns "funktionalitetsskydd" och vilken skyddstyp innebär att endast godkända eller certifierade program får och kan användas i systemet vid bearbetning av data.

Det skall noteras att denna skyddstyp fortfarande, i enlighet med uppfinningen, ligger på termnivå.

Antag i illustrerande syfte att Funk2 i termskyddskatalogen TK i fig 4 svarar mot detta skyddsattribut och att termer med termnamnet TN1 respektive TN2 endast får bearbetas med de godkända applikationerna eller programmen P1 respektive P2. Otillbörlig hantering av motsvarande termer med exempelvis ett annat program P3, eller en modifierad version P1' av P1, skall förhindras. Som skyddsattribut i termskyddskatalogen lagras därför data som identifierar P1 och P2. I ett föredraget exempel skapas, på ett i sig känt sätt, en kryptografisk checksumma P1* respektive P2* utifrån varje godkänt program P1 respektive P2. Dessa checksummor kan anses utgöra ett unikt fingeravtryck av respektive godkänt program, och dessa fingeravtryck kan lagras som skyddsattribut i termskyddskatalogen såsom illustreras schematiskt i fig 4. Det skall dock noteras att dylika checksummor för godkända program eventuellt kan lagras i en egen termskyddskatalog för registering av godkända program, separat från termskyddskatalogen med skyddsattribut för krypteringsstyrka.

Om sistnämnda skyddstyp "skyddade program" används, skall det också noteras att systemet, vid en användarinitierad åtgärd som syftar till bearbetning av en given term, exempelvis inskrivning av ett nytt termvärde i en viss post, inte behöver utföra någon komplett genomgång av alla i systemet godkända program. Om användaren exempelvis försöker använda ett program P3 för att i den operativa databasen O-DB skriva in ett nytt termvärde, så sker det ett tvingande anrop till termskyddskatalogen vid motsvarande termnamn, säg TN1. Från termskyddskatalogen inhämtas därvid tillhörande skyddsattribut P1*, vilket innebär att ett dylikt termvärde endast får lagras med programmet P1. Försöket att registrera term-

värdet med hjälp av programmet P3 skulle därför misslyckas.

Genom periodisk användning av ovan beskrivna funktionalitetsskydd kan man avslöja och/eller förhindra att en obehörig person (exempelvis en "hacker") med hjälp av ett icke godkänt program gör intrång i systemet och modifierar och/eller lägger till beskrivande data på ett sådant sätt att det beskrivande datat därefter blir identifierande för posten. Termvärdena får alltså inte bli identifierande i den operativa databasen O-DB.

Spårbarhet/Loggning

"Loggning" eller "spårbarhet" är en annan skyddstyp som enligt uppfinningen kan kopplas till ett termnamn i termskyddskatalogen. Om detta skydd är aktiverat för ett visst termnamn, kommer varje bearbetning av motsvarande termvärden i den operativa databasen O-DB att automatiskt och tvingande medföra att relevanta uppgifter om bearbetningen ("användare", "datum", "post", "användarprogram", etc) loggas på lämpligt sätt, så att man i efterhand utifrån loggen enkelt kan undersöka vem som har bearbetat de aktuella termvärdena, när, med vilket program, etc.

Läsning av data från den operativa databasen O-DB

Vid en användariniterad åtgärd som syftar till läsning/ändring av termvärden i de lagrade posterna i den operativa databasen O-DB, utförs nedan angivna steg åtgärder, vilka speciellt också innefattar ett tvingande anrop till termskyddskatalogen och en "uppackning" av datat som styrs automatiskt och tvingande av inhämtade skyddsattribut.

Steg 1 Posten identifieras genom framtagning av aktuell lagringsidentitet LID utifrån den originalidentitet OID (Pnr) som hör till det termvärde

TV som skall läsas, enligt följande:

$F_{KR}(F_{EIR}(OID)) = LID$

Steg 2 När posten är funnen medelst LID, dekrypteras det krypterade termvärdet TV (dvs det krypterade beskrivande data som skall läsas) enligt följande medelst en dekrypteringsalgoritm F_{DKR}:

$F_{DKR}(TV) =$ beskrivande data (klartext)

Genomförandet av denna dekryptering av termvärdet kräver dock att termens krypteringsstyrande skyddsattribut först inhämtas av systemet från termskyddskatalogen TK, dvs det attribut som anger med vilken styrka eller nivå som det i O-DB lagrade termvärdet TV har krypterats. I likhet med ovanstående procedur för inskrivning av data i O-DB föreligger det sålunda även vid läsning ett tvingande anrop till termskyddskatalogen TK för inhämtning av information som är nödvändig för att bearbetningen, här uppackningen, skall kunna genomföras.

Det inses att ett sådant tvingande anrop till termskyddskatalogen TK, vid försök till läsning, kan medföra att försöket helt eller delvis misslyckas av flera orsaker, i beroende av aktuella skyddsattribut som är kopplade till den eller de termvärden som skall läsas. Exempelvis kan försöket till läsning avbrytas på grund av att användaren försöker utnyttja ett icke godkänt program och/eller att denne icke är behörig att läsa den aktuella termen.

För det fall termskyddskatalogen är krypterad kan avkodningsnyckeln vara lagrad på en från den första och den andra databasen skild lagringsposition.

Fig 5 visar ett exempel på ett användargränssnitt i form av en dialogruta, med vars hjälp IAM-ansvarig, dvs en person som är säkerhetsansvarig, kan avläsa och/eller ändra de i termskyddskatalogen angivna skyddsattributen. I exemplet i fig 5 har termnamnen "Bostadsbidrag" och "Socialbidrag" båda försetts med skyddsattribut avseende kryptering, gallring, loggning och ägare. Vidare har, i undermenyer, registrering skett av auktoriserade aktörer och skyddade program kopplade till termnamnet "Socialbidrag".

PATENTKRAV

1. Metod för bearbetning av data som skall skyddas, innefattande åtgärden att lagra datat som krypterade termvärden (TV) hos poster (P) i en första databas (O-DB), varvid varje termvärde är kopplat till ett motsvarande termnamn (TN), k ä n n e t e c k n a d av:

att i en andra databas (IAM-DB) lagra en termskyddskatalog (TK), som för varje enskilt termnamn (TN) innehåller ett eller flera skyddsattribut som anger bearbetningsregler för termvärden (TV) som i den första databasen (O-DB) är kopplade till det enskilda termnamnet (TN),

att vid varje användarinitierad åtgärd, som syftar till bearbetning av ett givet termvärde (TV) i den första databasen (O-DB), initialt åstadkomma ett tvingande anrop till termskyddskatalogen för inhämtning av det eller de skyddsattribut som hör till motsvarande termnamn, och

att tvingande styra användarens bearbetning av det givna termvärdet i överenstämmelse med det eller de inhämtade skyddsattributen.

2. Metod enligt krav 1, vidare innefattande åtgärden att lagra termskyddskatalogens (TK) skyddsattribut i krypterad form i den andra databasen (IAM-DB), och att vid inhämtning av skyddsattribut från termskyddskatalogen (TK) åstadkomma en avkodning därav.

3. Metod enligt något av de föregående kraven, varvid varje post (P) i den första databasen (O-DB) har en postidentifierare, och varvid metoden vidare innefattar åtgärden att lagra postidentifieraren i krypterad form (LID) i den första databasen (O-DB).

4. Metod enligt något av de föregående kraven, varvid krypteringen av data i den första databasen (O-DB) och/eller krypteringen av data i den andra databasen (IAM-DB) utförs i enlighet med PTY-principen med flytande lagringsidentitet.

5. Metod enligt något av de föregående kraven, varvid termnamnens skyddsattribut innefattar attribut som anger regler för kryptering av motsvarande termvärden i den första databasen (O-DB).

6. Metod enligt något av de föregående kraven, varvid termnamnens skyddsattribut innefattar attribut som anger regler för vilket eller vilka program eller programversioner som får användas för hantering av motsvarande termvärden i den första databasen (O-DB).

7. Metod enligt något av de föregående kraven, varvid termnamnens skyddsattribut innefattar attribut som anger regler för loggning av motsvarande termvärden i den första databasen (O-DB).

SAMMANDRAG

Uppfinningen avser en metod för bearbetning av data som skall skyddas, innefattande åtgärden att lagra datat som krypterade termvärden (TV) hos poster (P) i en första databas (O-DB), varvid varje termvärde är kopplat till ett motsvarande termnamn (TN). Metoden kännetecknas av åtgärderna att i en andra databas (IAM-DB) lagra en termskyddskatalog (TK), som för varje enskilt termnamn (TN) innehåller ett eller flera skyddsattribut som anger bearbetningsregler för termvärden (TV) som i den första databasen (O-DB) är kopplade till det enskilda termnamnet (TN), att vid varje användarinitierad åtgärd, som syftar till bearbetning av ett givet termvärde (TV) i den första databasen (O-DB), initialt åstadkomma ett tvingande anrop till termskyddskatalogen för inhämtning av det eller de skyddsattribut som hör till motsvarande termnamn, och att tvingande styra användarens bearbetning av det givna termvärdet i överenstämmelse med det eller de inhämtade skyddsattributen.

Publiceringsbild: Fig 4

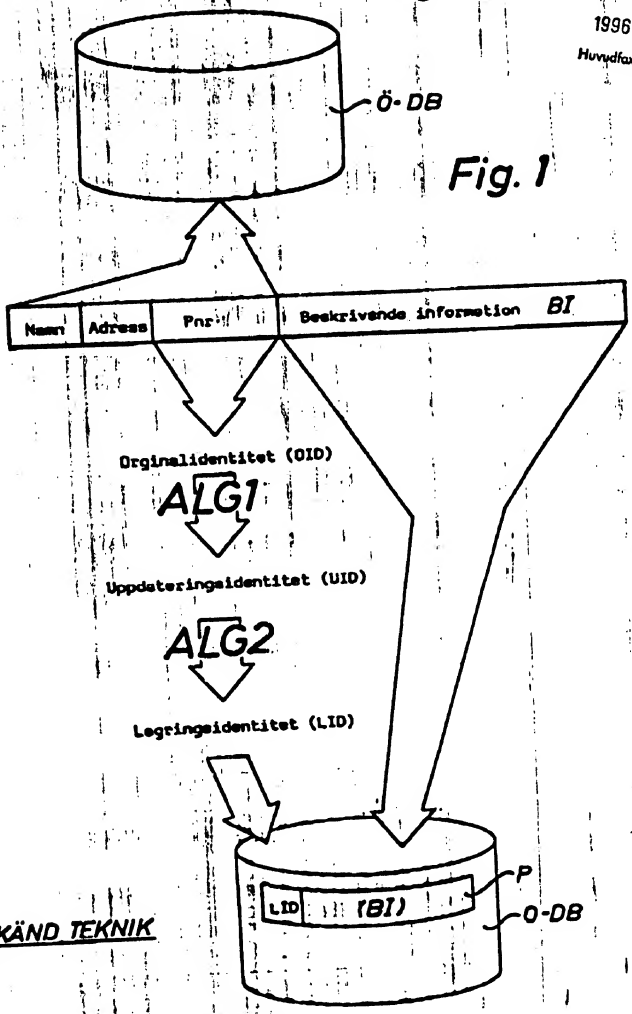

Fig. 1

KÄND TEKNIK

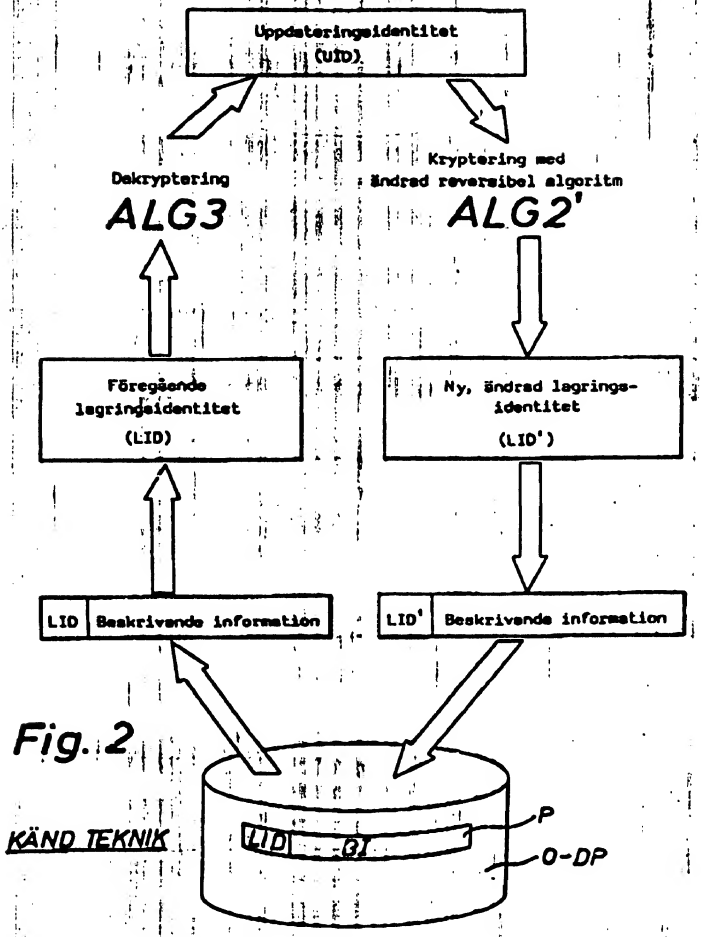

Fig. 2

KÄND TEKNIK

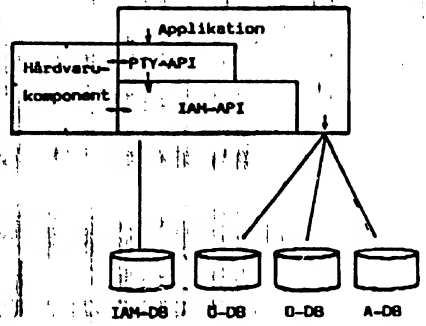

Fig. 3

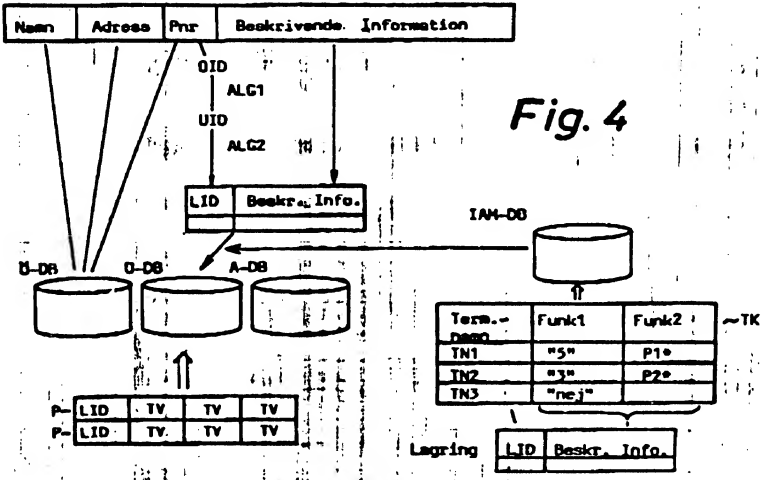

Fig. 4

IAM - Termkatalog - Operativ miljö

Termnamn	Kryptering	Gallringskod	Loggning	t.o.m.	Ägare
Bostadsbidr	Nej	4	60 dgr	Nej	Stig Svensson
Socialbidrag	Ja	4	60 dgr	Ja	951205 Stig Svensson

Aktörer

Tr

Socialbidrag

Auktoriserade aktörer

Ekonomichef E001 -
Controller C004

Spara

Avbryt

Socialbidrag

Trusted processes

PgmA001 v0103
PgmB002 v0201

Spara

Avbryt

Fig. 5